CLAIMS:

1. System for selective data transmission with
   - a sender (S)
   - and at least a first and a second receiver (R1, R2),
   - with encryption means (24) associated with said sender (S), said encryption means (24) comprising a plurality of base keys (k1, k2, k3, k4),
   - a transmission channel (C) from said sender (S) to said receivers (R1, R2) for transmission of encrypted data (42, 52, 62, 106),
   - and with decryption means (34) associated with each of said receivers (R1, R2), said decryption means (34) each comprising a receiver set of keys, where each receiver set of keys is a subset of said base keys (k1, k2, k3, k4),
   - where for transmission of data (40) at least to said second receiver (R2), said encryption means (24) are configured to encrypt said data (40) recursively with at least two keys (k1, k3, k4), said keys being comprised in said receiver set of said second receiver (R2), and at least one of said keys (k4) not being comprised in said receiver set of said first receiver (R1),
   - and were said decryption means (34) of said second receiver (R2) are configured to decrypt said data (42, 52, 62, 106) recursively with said at least two keys (k1, k3, k4).

2. System according to claim 1,
   - said system (10) further comprising a third receiver (R3) with decryption means (34.3) comprising a receiver set of keys which is a subset of said base keys (k1, k2, k3, k4)
   - where said receiver sets of said first, second and third receiver (R1, R2, R3) are pairwise different,

- and where said receiver set of said second receiver (R2) and said receiver set of said third receiver (R3) comprise at least two common keys (k1, k4) where at least one of said at least two common keys (k1, k4) is not comprised in said receiver set of said first receiver (R1),
- and where for transmission of data (40) to a group at least comprising said second receiver (R2) and said third receiver (R3), said encryption means (24) are configured to encrypt said data (40) recursively with at least said two common keys (k1, k4),
- and where said decryption means (34.2, 34.3) of said second and third receiver (R2, R3) are each configured to decrypt said data (42, 52, 62, 106) recursively with at least said two common keys (k1, k4).

3. System for selective data transmission according to one of the above claims with
   - a plurality of receivers (R1, R2, R3, R4), each with associated decryption means (34) with a receiver set of keys, where said receiver sets are pairwise different,
   - where an authorized group of said receivers (R2, R3) is authorized to receive said data,
   - and where for transmission of said data (40) to the receivers of said authorized group, said encryption means (24) are configured to encrypt said data (40) recursively with a plurality of keys (k1, k4), all of said keys being comprised in said receiver sets of the receivers of said authorized group, and for each receiver not belonging to said authorized group (R1), at least one of said keys not being comprised in the corresponding receiver set,
   - and were said decryption means (34) of the receivers of said authorized group (R2, R3) are configured to decrypt said data (42, 52, 62, 106) recursively with said plurality of keys (k1, k4).

4. System according to claim 3, where
   - said authorized group of receivers is divided into at least two subgroups,
   - and for transmission of said data (40) to the receivers of said authorized group, said data is transmitted to said receivers in at least two transmissions, where in

each transmission the data is encrypted recursively with a different set of keys, all of said keys being comprised in said receiver sets of the corresponding sub-group of receivers.

5. System according to one of the above claims, where
   - said encryption means (24) are configured for recursive encryption with a plurality of encryption steps, where in each encryption step a piece of data (D) is encrypted with a key (k1) to calculate an encrypted piece of data (D1),
   - where each of said encryption steps includes calculation of at least one exponentiation with a key number associated with said key (k1),
   - said encryption means being configured to recursively apply said encryption steps with a plurality of keys (k1, k2... kn) by multiplying key numbers associated with said keys, and calculating an exponentiation with the result of said multiplication.

6. System according to one of the above claims, with
   - a plurality of receivers,
   - where said receivers are divided into a plurality of groups (90a, 90b),
   - where for each of said groups (90a, 90b), the encryption means (24) comprise a group set of base keys, said group sets being pairwise different from each other,
   - and the decryption means (24) of each of said receivers comprise a receiver set of keys, which is a subset of the group set of the group that the respective receiver is a member of.

7. System according to one of the above claims, with
   - a plurality of receivers (R1-R4), with decryption means (34) associated with each of said receivers (R1-R4), said decryption means (34) each comprising a receiver set of keys, where each receiver set of keys is a subset of said base keys (k1-k4),

- where each of said receiver sets of keys comprises the same number of base keys.

8. System according to one of the above claims, with
   - a plurality of receivers,
   - and storage means associated with said sender (S) which store information about a first, authorized group of receivers out of said plurality of receivers, and/or about a second, unauthorized group of receivers out of said plurality of receivers,
   - where said sender (S) comprises distribution control means for controlling message transmission, said distribution control means being configured to determine one or more combinations of said base keys (k1-k4), such that messages recursively encrypted with said combinations are decryptable only at said receivers belonging to a first group, and are not decryptable at said receivers belonging to said second group.

9. System according to one of the above claims, with
   - a number k of base keys,
   - and a number N of receivers, and with decryption means associated with each of said receivers, said decryption means each comprising a receiver set of keys, where each receiver set of keys is a subset of said base keys,
   - where $\begin{pmatrix} k \\ m \end{pmatrix}$ each receiver set of keys contains a number m of said base keys,
   - where is substantially greater than N.

10. Sender for use in a transmission system according to one of the above claims, with
    - encryption means (24) comprising a plurality of base keys (k1-k4), said encryption means (24) being configured to encrypt data (40) recursively with at least two of said base keys (k1-k4),
    - and transmission means (26) for transmitting said encrypted data (D') over a transmission channel (C).

11. Receiver for use in a transmission system according to one of claims 1-9, with
    - receiving means (32) for receiving encrypted data (D') of a transmission channel (C),
    - and decryption means (34) comprising a receiver set of keys,
    - where said decryption means (34) are configured to decrypt said encrypted data (D') recursively with at least two of said keys.

12. Broadcasting system with
    - scrambling means (110) for scrambling content (F) with a scrambling key (m),
    - a broadcasting sender (Sb) for broadcasting said scrambled content (F') over a channel,
    - said broadcasting system further comprising a selective data transmission system according to one of claims 1-9 with a sender (S) and receivers (R1-R4) for selectively transmitting the scrambling key (m),
    - where said receivers (R1-R4) each comprise de-scrambling means (112) for de-scrambling said scrambled content (F') with said scrambling key (m).
    -

13. Method for selective data transmission, where encrypted data is transmitted
    - from a sender (S) comprising a plurality of base keys (k1-k4),
    - to at least a first and a second receiver (R1, R2), each comprising a receiver set of keys, where each receiver set of keys is a subset of said base keys (k1-k4),
    - where for selective transmission of data two set second receiver (R2) said method includes the following steps:
        - at said sender (S), encrypting said data (40) recursively with at least two keys (k1, k3, k4), said keys (k1 k3, k4) being comprised in said receiver set of said second receiver (R2), and at least one of said keys (k4) not being comprised in said receiver set of said first receiver (R1),
        - transmitting the encrypted data (42, 52, 62) over a transmission channel (C),
        - and, at said second receiver (R2), decrypting said encrypted data (42, 52, 62, 106) recursively with said at least two keys (k1, k3, k4).

14. Method according to claim 13, said method further comprising the steps of
    - determining at least one base key (k1, k2, k3, k4) to exchange,
    - generating at least one new base key,
    - encrypting the new base key recursively with a plurality of base keys, and transmitting the thus encrypted key to a plurality of receivers.

15. Method for operating a system including a sender (S) and a plurality of receivers (R1-R4), said method comprising the steps of
    - determining an issuing scheme for issuing a number of base keys (k1-k4) to a number of receivers (R1-R4), where each of said receivers (R1-R4) holds a number of said base keys (k1-k4),
    - generating said base keys (k1-k4),
    - and, upon joining of said receivers (R1-R4), distributing said base key (k1-k4) to said receivers (R1-R4) according to said predetermined issuing scheme.